Refine Search

Search Results -

Terms	Documents
L32 and (authentication with record or authentication near record or authentication adj record)	175

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text | Clear | Interrupt

Search History

DATE: Tuesday, August 01, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L33	L32 and (authentication with record or authentication near record or authentication adj record)	175	L33
L32	L31 and (data with process$ or data near process$ or data adj processing)	1023	L32
L31	L30 and (finance or financial or financ$) with transaction	1150	L31
L30	(authentication or authenticate) and (authorization or authorizat$) and accounting	5593	L30
L29	l20 and 705/44	25	L29
L28	l27 and 705/44	15	L28
L27	L26 and (data with process$ or data near process$ or data adj process$)	72	L27
L26	L21 and 705.clas.	78	L26
L25	L22 and 705.clas.	22	L25
L24	L22 and 705/44	12	L24

L23	L22 and (database or data with base or data adj base) and (store or storage or stor$)	27	L23
L22	L21 and (account with holder or account near holder or account adj holder)	33	L22
L21	L20 and (match or match$)	307	L21
L20	L19 and (predict or prediction) and amount and time and signature	326	L20
L19	L18 and (authentication or authenticate) and (record or file)	3992	L19
L18	L17 and (secure or security or encrypted or encryption or encrypt)	11464	L18
L17	(financial near transactions or financial with transactions or financial adj transactions)	19092	L17
DB=USPT; PLUR=YES; OP=OR			
L16	'5754654'.pn.	1	L16
L15	'5568552'.pn.	1	L15
L14	'5511121'.pn.	1	L14
L13	'6336095'.pn.	1	L13
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L12	6812938.pn.	2	L12
DB=USPT; PLUR=YES; OP=OR			
L11	'5161190'.pn.	1	L11
L10	'5719841'.pn.	1	L10
L9	'5920879'.pn.	1	L9
L8	'5506905'.pn.	1	L8
L7	'4868877'.pn.	1	L7
L6	'5987133'.pn.	1	L6
L5	'5537475'.pn.	1	L5
L4	'5537475'.pn.	1	L4
L3	'5987133'.pn.	1	L3
L2	'5987133'.pn.	1	L2
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L1	6141751.pn.	2	L1

END OF SEARCH HISTORY

Freeform Search

Database: US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Term: (automated near authentication and authorization and accounting or automated with authentication and authorization and accounting or automated adj

Display: 10 **Documents in Display Format:** - **Starting with Number** 1

Generate: ○ **Hit List** ◉ **Hit Count** ○ **Side by Side** ○ **Image**

Search Clear Interrupt

Search History

DATE: Tuesday, August 01, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L22	5821933.pn.	2	L22
L21	5177789.pn.	2	L21
L20	"mizrah, len".in.	15	L20
L19	L18 and signature	26	L19
L18	L17 and time	34	L18
L17	L16 and amount	34	L17
L16	L15 and (financial with transaction or financial near transaction or financial adj transaction)	36	L16
L15	(automated near authentication and authorization and accounting or automated with authentication and authorization and accounting or automated adj authentication and authorization and accounting)	69	L15
L14	902/22	218	L14
L13	902.clas.	2152	L13
L12	707/100	8421	L12
L11	707.clas.	36543	L11

L10	705.clas.	43574	L10
L9	705/79	225	L9
L8	705/75	554	L8
L7	705/50	557	L7
L6	705/44	1143	L6
DB=USPT; PLUR=YES; OP=OR			
L5	'5963649'.pn.	1	L5
L4	'5970145'.pn.	1	L4
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L3	6085320.pn.	2	L3
L2	6233565.pn.	2	L2
L1	6282656.pn.	2	L1

END OF SEARCH HISTORY

L19: Entry 21 of 26 File: USPT Sep 11, 2001

DOCUMENT-IDENTIFIER: US 6289323 B1
** See image for Certificate of Correction **
TITLE: System and method for completing monetary transactions by presentment of postage value to a postal authority

Brief Summary Text (2):
The present invention generally relates to a method and system for paying for goods, services, etc. in a manner similar to checks, credit cards, and debit cards. More particularly the present invention relates to the use of cryptographically transformed user information to authenticate payments from a payer to a payee wherein the form of payment is a value message bearing, in addition to the typical information on a check, cryptographically transformed information including a digital signature for purposes of authenticating the value message. The value messages are authenticated and debited/credited to the payer/payee.

Brief Summary Text (4):
Bank checks have been used for centuries to conduct "cashless" transactions, and involve the submission of a signed negotiable instrument in exchange for a product or service of value to the payer. Bank checks, while convenient, do have certain drawbacks since they can be easily forged and fraudulently endorsed by parties other than the intended recipients. As a result, a whole body of rules, regulations and restrictions--including delays in clearing bank checks for multiple days--has developed to deal with the inherent flaws in this system which relies upon an easily defeated form of authentication, a handwritten signature.

Brief Summary Text (5):
In this age of high technology, electronic funds transfers are becoming more and more prevalent and come in many forms. Credit cards are now more widely used. Automatic bill payment is the chosen means for many homeowners to pay the monthly mortgage and utility bills. Debit cards are similar to credit cards. However, the amount of a debit card transaction is taken immediately from a payer's corresponding bank account. A "smart" card is similar to a debit card except that value is stored within a smart card and therefore a user need not have a separate bank account from which funds are taken when a debit transaction occurs. A smart card is essentially a self-contained electronic wallet or purse.

Brief Summary Text (6):
Notwithstanding the advantages of electronic transactions, these methods continue to suffer from several drawbacks. One is authentication. Debit and credit cards continue to rely upon handwritten signatures.

Brief Summary Text (10):
In accordance with the present invention, a party wishing to make a purchase creates a value message using a postal authority postage evidencing/accounting device. The value message includes payer identification, payee identification and a value amount. The value message is then "signed" by the payer by generating and appending a digital signature to the value message. Upon presentation of the value message to a postal authority outlet, the value message is authenticated by applying a public key to the digital signature. Upon successful authentication of the digital signature, an account status is adjusted to reflect successful

completion of negotiating the value message.

Brief Summary Text (11):
In accordance with another aspect to particular embodiments of the invention, parties using the postage accounting device can preserve privacy when making purchases from a merchant. A user submits a purchase order in the form of a value message to the merchant. The merchant ships the purchased goods with indicia including an identification number corresponding to the anonymous customer. The postal authority resolves the customer identification into an address.

Detailed Description Text (2):
Turning to FIG. 1, a schematic depiction is provided of a system incorporating the present invention. To simplify the description, the invention is described with reference to a single customer and merchant transaction. However, it will be appreciated by those skilled in the art that the present invention is used in a multiple customer/merchant environment. The postal authority 10, through its local outlets, performs initialization and finance/accounting operations relating to Payer Postal Security Device (PSD) 12 possessed by a person having an account with the postal authority. The Payer PSD 12 issues a value message 14 in exchange for goods and/or services. The merchant endorses the value message 14 by means of a Payer PSD 16 to render an endorsed value message 17. Thereafter, the merchant presents the endorsed payment PSD 17 to the postal authority 10. The postal authority 10, authenticates the value message and then credits the account of the Payee PSD 16 and registers the completed transaction in the account of the payer, the possessor of the Payer PSD 12.

Detailed Description Text (3):
The Payer PSD 12 is a secure register for evidencing/tracking value. In one implementation of the present invention, a possessor of the Payer PSD 12 deposits funds in advance with the postal authority. The possessor of the Payer PSD 12 then establishes a communication link enabling the postal authority or an intermediary (such as a postage evidencing device vendor) to request the postal authority to provide a value download message to the Payer PSD 12. The postal authority 10 issues a value download message to the Payer PSD 12 instructing the Payer PSD 12 to increase an internal account status register by an amount less than or equal to the amount transferred to the postal authority 10. The Payer PSD 12 will not issue value message value that exceeds the amount of available funds maintained within a local register of the Payer PSD 12. Such a system for limiting issuing value ensures that a user will not exceed the funds allocated to the Payer PSD 12. When used as a credit dispensing device, the Payer PSD 12 ensures that the user's disbursements of value message value do not exceed the credit left in the account, a value stored in secure internal registers within the Payer PSD 12. When used as a credit device, the internal registers ensure that the user's disbursements of value message value do not exceed the authorized credit limit. The Payer PSD 12 also includes the capability to log Payer PSD recharge operations and value message disbursements for purposes of auditing or verifying disbursements.

Detailed Description Text (4):
In yet another embodiment of the invention, the Payer PSD 12 is utilized as a secure signature device, but the user is not limited by an amount stored in a "rechargeable" value register. The user's transactions are merely registered at the postal authority and forwarded to the user's designated account which could be, for example, a credit card account or checking account.

Detailed Description Text (7):
Regardless of the form, the value message includes both text fields and encoded graphics such as one-dimensional or two-dimensional barcode graphics symbols. The value message is similar to, yet includes several variations from, the graphically encoded indicia of the known Information Based Indicia Program (IBIP) Performance Criteria for Information-Based Indicia and Security Architecture for IBI Postage

Metering Systems (PCIBISAIBIPMS) published by the postal authority Aug. 19, 1998, the contents of which are incorporated by reference in their entirety. The text fields include a payer identification, a payee identification, a value assigned the value message by the payee, and a time/date that the value message was issued by the payee. The text fields will be described herein below in conjunction with a description of FIG. 2.

Detailed Description Text (8):
When the value message is placed on a paper media, the encoded graphics portion of the value message 14 includes barcode graphics corresponding to the above described text fields as well as additional information that is only provided in graphical barcode form. Digital barcode encoding the text fields facilitates processing value messages automatically without reliance upon character recognition technology that can be less reliable. Barcode graphics also provide a useful format for employing digital signature cryptographic transformations to establish the authenticity of value messages. The value message 14 is digitally signed by the Payer PSD 12 using a digital signature that is a function of the above described text fields. The payer digital signature, encoded using a private key and in accordance with well known public/private key cryptographic transformation schemes, is used to authenticate, with a very high level of reliability, the Payer PSD 12 from which the value message 14 was issued. Because the digital signature is based upon the data fields of the value message 14, it also ensures that none of the data fields have been altered.

Detailed Description Text (9):
In exchange for providing goods and/or services, the Payer PSD 12 issues the value message 14 to a merchant. After receiving the value message 14, the merchant endorses the value message 14 using a Payee PSD 16. The result of the endorsement process is the endorsed value message 17. During the endorsement process the merchant adds additional data (discussed further below) and then renders a second digital signature which is based upon data fields contained in the endorsed value message 17. Thus, in addition to the above fields found on the value message 14, the endorsed value message 17 includes data fields added by the Payee PSD 16. The added fields include a payee digital signature which is rendered in graphical barcode format on the endorsed value message 17. The payee digital signature, in combination with a Payee PSD identification, enables the postal authority 10 to authenticate the payee. Information fields of the value message 14 and endorsed value message 17 set forth above will be described in greater detail with reference to FIG. 2.

Detailed Description Text (10):
Continuing with the general description of FIG. 1, the merchant presents the endorsed value message 17, issued by the Payee PSD 16, to the postal authority 10. A barcode graphics scanner/decoder at the postal authority 10, or some other remote location communicatively linked to the postal authority 10, reads the encoded barcode graphics of the endorsed value message 17 and renders a set of binary data corresponding to the encoded digital information and digital signature. The postal authority 10 applies a public key corresponding to the decoded digital signature barcode graphics provided by the Payer PSD 12 and the Payee PSD 16 to authenticate a cryptographically created digital signatures. Thereafter the postal authority 10 compares the digital signatures to a second set of data obtained from the endorsed value message 17. If the public key cryptographically transformed digital signature matches the second set of data (e.g., a hashed version of information fields within the endorsed value message 17), then the postal authority 10 concludes that the endorsed value message 17 is authentic.

Detailed Description Text (15):
In accordance with a specific example of a debit instruction model for payment, the postal authority 10 processes authenticated endorsed value messages in a manner similar to the manner in which presented bank checks are processed. The postal

authority 10 credits the account of the merchant/payee identified in the endorsed value message 17 and logs the presentation of the endorsed value message 17 within the account associated with the Payer PSD 12. Since value is not actually deducted from an account when the Payer PSD 12 is funded (the value has not been issued by the Payer PSD 12 nor has it been presented by a payee), the value of the endorsed value message 17 is subtracted from the payer's account. As noted previously above, the Payer PSD 12 may be used as a debit or credit device. In such instances, the postal authority 10 forwards the transaction to an appropriate financial institution.

Detailed Description Text (17):
Turning to FIG. 2, the fields of a value message are summarized in chart format. A first column identifies a particular data element represented on the value message. A second column specifies whether the data element identified in column 1 is provided in the barcode graphics portion of the value message. A third column specifies whether the data element identified in column 1 is also represented in text form. The length of the data elements range from 1 byte to over one hundred bytes. The largest field, an RSA digital signature, is 128 bytes. It is noted, however, that the choices for the lengths of various data fields are design considerations and do not limit the claimed invention. It is further noted that while several data element are identified in FIG. 2, others may be added without deviating from the invention.

Detailed Description Text (18):
A first group of data elements enables the postal authority 10 to perform certain initial inquiries to determine how to interpret a received endorsed value message. A version 30, provided in barcode form only, identifies the version of the indicia printed on the value message to ensure that the barcode graphics are properly decoded/interpreted by the postal authority 10. Next, an algorithm ID 32, provided in barcode form only, identifies the type of cryptographic transformation algorithm used to render the payer digital signature. Examples of such algorithms are Digital Signature Algorithm (DSA); Rivest, Shamir, Adelman (RSA); and Elliptical Curve Digital Signature Algorithm (ECDSA). A PSD certificate serial number 34, provided in barcode form only, identifies the serial number for the certificate used to authenticate the public/private key combination issued to the Payer PSD 12 by a Certificate Authority. The PSD certificate serial number 34 enables the postal authority 10 to select a public key from a public key database maintained by the postal authority 10. The public key corresponds to a private key used by the Payer PSD 12 to create a digital signature for the value message 14. Thus, the Payer PSD 12 need not include the public key with the value message 14.

Detailed Description Text (19):
The next set of data elements facilitate tracking value messages and accounting. A device ID 36, provided in both text and barcode form, represents the unique identifier of the Payer PSD 12 (i.e., each instance of a payer PSD receives its own unique identification). The device ID 36 in an embodiment of the present invention, is the payer identification. Embedded within the device ID 36 is a provider ID that specifies the maker of the Payer PSD 12, a model identification, and a device serial number (for the particular provider and model). In other embodiments, additional fields are provided which enable a specific user of the Payer PSD 12 to be identified as the payer. For example fields identifying the payer's name and identification number. In such instances, additional safeguards may be added, such as personal identification numbers (PINs) to ensure that the value of a processed endorsed value message is subtracted from one of potentially several accounts that may use the Payer PSD 12.

Detailed Description Text (20):
An ascending register value 38, provided in barcode form only, specifies a running accumulated total of the value dispensed by the Payer PSD 12. The ascending register starts at zero and is incremented by the value assigned to the value

message each time the Payer PSD 12 issues a new value message. A descending register value 40, provided in barcode form only, specifies the amount of money/credit left in the Payer PSD 12 after decrementing the descending register by the value specified by the value message 14. The descending register 40 acts as a safeguard against another unauthorized user obtaining access to the Payer PSD 12 and cleaning out the entire account of the rightful owner of the PSD 12. The descending register 40 can be loaded with the full amount of value/credit remaining in the corresponding account, but the descending register 40 may also be loaded with a smaller amount specified by the PSD 12 during a funding operation. During a funding operation a user requests additional value to be added to the Payer PSD 12, and in response the descending register value 40 is increased by the requested amount. When the Payer PSD 12 is used as a credit/debit device, the descending register need not be used, or used alternatively to impose a credit limit upon the Payer PSD 12.

Detailed Description Text (21):
A payment value 42, provided in both text and barcode form, specifies the amount that the value message 14 is worth when presented to the postal authority 10. When the value message is processed by the postal authority 10, the payee's account is credited by the amount specified by the payment value 42, and the payer's account is debited by an equal amount.

Detailed Description Text (22):
The value message 14 includes a date/time 44 corresponding to when the value message was issued by the Payer PSD 12. The date/time 44, provided in both text and barcode form, may be used by the postal authority 10 to generate detailed transaction reports for the Payer PSD 12. The date/time 44 may also be used to impose limitations on the presentation of "stale" value messages. Since the value message negotiation process is completely automated, flexible rules may be applied to the presentation of "stale" value messages. For example, a particular company may be offering rebates from the Payer PSD 12 with a requirement that all rebates must be received within 30 days of issuance. The postal authority 10, upon receipt of a value message, identifies the time limit from its database (or from a field on the value message) and accepts the value message if it has been presented within the required 30 days.

Detailed Description Text (23):
The value message, as mentioned above, includes a payee identification 46. The payee identification 46, provided in both text and barcode form, specifies an account to which the postal authority 10 applies a deposit/credit in the amount specified in the payment value 42 when the value message is processed. The payee identification uniquely identifies a payee account. Since personal names, such as "John Smith" may be duplicated, the payee identification includes a unique alphanumeric account identification.

Detailed Description Text (25):
The data segment that will be discussed is a payer digital signature 50. In an embodiment of the invention, the payer digital signature 50, provided in barcode form only, is a hashed, cryptographically transformed representation of all the data fields set forth above. As a result, if a recipient of the value message were to change any data element, the digital signature would no longer correspond to the data fields. In that case, when the value message is presented to the postal authority 10 and the value message is processed, the authentication of the value message would fail and the presented endorsed value message 17 would be rejected. The payee digital signature 50 thus not only provides highly reliable tracing of the source of the digital signature 50 to the Payer PSD 14, the digital signature 48 presents a virtually insurmountable barrier to persons who may attempt to modify either the amount or payee specified in the value message 14.

Detailed Description Text (26):

The endorsed value message 17 includes a set of additional fields for authentication and record keeping. An algorithm ID 52, provided in barcode form only, identifies the type of cryptographic transformation used to render a payee digital signature 54 appended by the Payee PSD 16 when the endorsed value message 17 is issued by the Payee PSD 16. The payee digital signature 54 is cryptographically transformed by means of a public key stored at the postal authority 10 and accessed based upon the payee identification 46. Finally, the endorsed value message 17 includes a date/time 56 which specifies when the Payee PSD 16 issued the endorsed value message 17.

Detailed Description Text (29):
The steps for carrying out a Payer PSD funding operation are summarized in FIG. 3. At step 100, the Payer PSD 12 issues a request to the postal authority 10 for a specified value to be funded to the Payer PSD 12 by the postal authority 10. The request includes a PSD identification and a private key cryptographically created digital signature. At step 102, the postal authority 10 authenticates the funding request from the Payer PSD 12 by cryptographically transforming the digital signature using a public key corresponding to the Payer PSD 12. The postal authority 10 also determines whether the amount requested by the Payer PSD 12 can be provided without exceeding the account limit for the Payer PSD 12.

Detailed Description Text (31):
Next, at step 106 the postal authority 10 issues a value download message to the Payer PSD 12. The value download message is authenticated with a private key cryptographically rendered digital signature. At step 108, the Payer PSD 12 cryptographically transforms the digital signature using a public key provided to the Payer PSD 12. The authenticated value download message is then used to increase the descending register value in the Payer PSD 12 by an amount equal to the funded amount.

Detailed Description Text (33):
If at step 202, the user has entered a valid PIN for the entered payer identification, then control passes to step 212 wherein an amount is entered for the value message 14. Control then passes to step 214 wherein the Payer PSD 12 determines whether a valid amount was entered. If an invalid amount was entered (i.e., the entered amount exceeds a prescribed limit), then control passes to step 216 wherein an error message is generated indicating that the user has entered an invalid amount. Control returns to step 200 wherein the user must reenter an identification and PIN in order to retry entering a valid amount.

Detailed Description Text (34):
If at step 214 the amount specified by the user is valid, then control passes to step 218 wherein the Payer PSD 12 accepts an identification for the intended payee for the value message. Having received all the necessary information, the Payer PSD 12 at step 220 applies the amount to the current values of the ascending and descending registers, generates a transaction number, logs the transaction, and generates a payer digital signature. Control then passes to step 222 and the Payer PSD 12 causes the value message 14 to be issued. Control then passes to Exit step 210, a wait state wherein the PSD 12 awaits a next transaction (e.g., funding, vending, auditing, etc.).

Detailed Description Text (36):
If at step 302, the user has entered a valid PIN for the entered payee identification, then control passes to step 312 wherein the Payee PSD 16 endorses the value message 14 by appending the payee digital signature to render the endorsed value message 17. Next, at step 314 the Payee PSD 16 issues the endorsed value message 17. As previously mentioned, the endorsed value message 17 is typically issued in paper form. However, it may also be issued in electronic form directly to the postal authority 10 without printing out the endorsed value message 17.

Detailed Description Text (37):
Turning now to FIG. 6, the steps are summarized corresponding to the stage of the value message life cycle wherein the endorsed value message 17 is negotiated. At step 400 the postal authority 10 scans the submitted endorsed value message 17 and converts the scanned barcode graphics to electronic digital data. Next at step 402 the postal authority 10 applies the payer public key to the payer digital signature. If, at step 404, the cryptographically transformed payer digital signature is not equal to a reference data string obtained by applying a hash function to data elements of the value message 14, then control passes to step 406. At step 406 the postal authority 10 rejects the endorsed value message 17 and logs the rejection transaction for purposes of later investigation of why the endorsed value message 17 was rejected. Control then passes to Exit step 408.

Detailed Description Text (38):
If, at step 404, the cryptographically transformed payer digital signature is equal to the reference data string, then control passes to step 410. At step 410 the postal authority 10 applies the payee public key to the payee digital signature. If, at step 412, the cryptographically transformed payee digital signature is not equal to a reference data string obtained by applying a hash function to data elements of the endorsed value message 17, then control passes to step 406. However, if the cryptographically transformed payee digital signature is equal to the reference data string generated from the endorsed value message 17, then control passes to step 414. At step 414 the postal authority 10 compares the issue date field of the endorsed value message 17 to the present date to determine whether the endorsed value message 17 is stale. If the endorsed value message 17 is stale, then control passes to step 406. If the endorsed value message 17 has been presented within the prescribed time period, then control passes to step 416 and the endorsed value message 17 is processed, and the accounts of the payee and payer are debited and credited respectively. At step 418 the transaction is logged for purposes of generating a monthly statement or auditing.

Detailed Description Text (39):
Turning now to FIG. 7, in another embodiment of the present invention, indicia and cryptographic transformations are incorporated into an electronic commerce transaction between a merchant and an anonymous customer. FIG. 7 illustratively depicts the stages of such a transaction. During stage 1 of the electronic commerce transaction, an e-commerce customer 500, using a postal security device (PSD) 501, generates a value message and transmits it to an e-commerce merchant 502 identifying a product that the customer 500 wishes to purchase. The product that the customer wishes to purchase is identified in the message/memo field 60 of the value message (see FIG. 2). The value message includes an identification of the PSD 501 issued to the customer 500. However, consistent with the intent to guard the privacy of the customer 500, the value message does not provide the identity of the customer 500 (e.g., no delivery address or email address). The value message, specifying an amount for the purchase identified in the message/memo field, is digitally signed by the payer PSD 12.

Detailed Description Text (40):
Next, at stage 2 of the e-commerce transaction, the e-commerce merchant 502, using a PSD 503, endorses the value message received from the customer 500. The endorsed value message includes the additional information and signature in fields 52, 54 and 56. In addition the merchant 502 may include a unique transaction value in the transaction identification 58 or a message to the postal authority 504--or an equivalent e-commerce clearinghouse. However, the unique transaction identification is preferably provided by the postal authority 504.

Detailed Description Text (41):
Next, at stage 3, the postal authority 504 performs cryptographic transformations upon the received endorsed value message to verify the authenticity of the

signatures. As mentioned above, the present invention can be adapted to virtually any transaction model (e.g., value token, credit instructions, debit instructions, etc.). In the case where the endorsed value message is a debit instruction, the postal authority 504 verifies that the customer 500 has sufficient funds available to carry out the transaction. If the value token model is used, the message itself is value and the postal authority 504 need not verify the availability of funds or whether a credit limit has been reached. However, the postal authority 504 may apply customized fraud/spendthrift policies when processing the endorsed value message. Such policies may include transaction limits and time-based limits (e.g., $1,000/day). In order to perform this check, the postal authority correlates the PSD identification in the endorsed value message to a customer account within the postal authority's confidential database of customer PSD ID's. The postal authority returns a transaction identification to the merchant 502 which serves as the authorization for the merchant to mail the product purchased by the customer 500.

Detailed Description Text (44):
The stages described below relate to delivery of the parcel to the electronic commerce customer 500. During stage 6 an email system 507 within the postal authority 504 sends email to the customer 500 informing the customer that the postal authority 504 has received a parcel from the merchant 502. The email address may be included within the indicia, or if the customer wishes to maintain anonymous to the sender, then the email address is determined by the postal authority 504 from a database based upon a customer alias provided in the indicia. The email includes any of a number of pieces of information. For example, the email message preferably contains a field identifying a delivery schedule for the parcel. The postal authority 504 may inform the user of a likely time and date for delivery of the parcel. Alternatively, if delivery is to a post office box, the email message notifies the customer that mail is waiting at the customer's post office box. The email may also include a message from the merchant 502 that was extracted by the postal authority 504 from the memo/field within the indicium on the parcel.

Detailed Description Text (45):
At stage 7, the customer 500 submits a reply to the email sent by the postal authority 504. The reply, in addition to referring to the email message previously sent by the postal authority 504, confirms the scheduled delivery or alternatively specifies an alternative date/time. Other messages submitted by the customer may request that the postal authority 504 hold the parcel at a local post office to be picked up by the customer 500. The email operation is described in greater detail herein below with reference to FIG. 8.

Detailed Description Text (47):
Having described particular example of an application of the value message and IBIP indicium specification for mail pieces which enable a customer to anonymously or pseudonymously conduct electronic commercial transaction with an e-commerce vendor, it will be appreciated by those skilled in the art that the above described stages may be modified while still allowing a user to submit a purchase request to a vendor in an e-commerce environment without revealing the customer's name, social security number, address, phone number, account codes, or other personal information that can be used for fraudulent or irritating actions at a later time by the e-commerce vendor or another company which purchases such information from the e-commerce vendor. Such other arrangements are intended to fall within the scope and spirit of the disclosed invention.

Detailed Description Text (49):
At step 600, the postal authority receives a parcel or piece of mail including graphically encoded indicia as specified in the postal authority indicia program incorporated herein above by reference. At step 602, the postal authority scans the indicia and decodes the graphically encoded information contained within the indicia. In addition to standard address, accounting and security information, the graphically encoded indicia may include a first optional field that is decoded by

the postal authority to determine an intended recipient of an email message. It is noted however, that the postal authority may determine the recipient in many cases by merely referring to the portion of the decoded information relating to the addressee of the scanned parcel. A memo/message field within the indicia contains a message from the sender of the parcel/mail piece. It is noted however that even when the memo/message field does not contain a message, the postal authority will transmit its own message informing the email recipient that the postal authority has received a parcel to be delivered to the email recipient.

Detailed Description Text (51):
At step 606 the postal authority transmits email to the recipient including a message concerning delivery instructions (e.g., time and/or date for delivery) and/or a message from the merchant which was extracted from indicia on the parcel. While the above sequence of steps would be tedious and time consuming if performed manually, in the preferred system these steps are performed automatically by an integrated system at the postal authority including a parcel indicia scanner and an automated email system including an email address database, automated email document editor, and email mailing/receiving system. In such an integrated system, the information needed for emailing the recipient is extracted from the decoded, scanned indicia. An email document is automatically generated by the postal authority email system without any human intervention. The completed email document is automatically sent. Furthermore, the email system can be expanded to provide for standardized forms and keyed to generate forms based upon such variables as: mail class, sender type, receiver type, etc. The automated email form generation system can be programmed to evaluate the variables and select a proper email form.

Detailed Description Text (52):
At step 608, the email system waits a period of time that can be interrupted by reception of a response from the recipient of the email. At step 610 the mail system determines whether a response has been received from the recipient of the previously sent email. If an email response was received, then control passes to step 612 and the postal authority email system 507 processes the response and schedules a time and point for delivery of the parcel. The time may be merely "as soon as possible" or a more specific period such as a particular hour of a specified date. The postal authority email system 507 confirms the returned email message by submitting yet another email message to the parcel recipient. At step 614, the parcel is delivered.

Detailed Description Text (56):
Referring to FIG. 2, fields 30, 32, 34, 36, 38 and 40 will refer to the vendor and the vendor's PSD rather than the sender of the postcard (the customer 704). Since the vendor 700 is paying the postage, the account registers 38 and 40 will correspond to the vendor's PSD. The payment value 42 will designate the amount to be paid by the customer 704 to the vendor 700.

Detailed Description Text (57):
As will be demonstrated below, it is not necessary for the customer 704 to have a PSD or other means for generating indicia to carry out the preferred version of bill payment. Therefore, in the preferred embodiment of the invention, the payer digital signature 50 is not utilized. However, in alternative embodiments requiring automated authentication of a payer's authorization to pay a bill, the payer digital signature 50 will be generated and added by the customer prior to placing the postcard in the mail stream. The vendor 700 generates and inserts a digital signature into the payee digital signature 54. The customer 704, in addition to being identified on the postcard in text form, is identified in the message/memo field 60. Finally, because it is envisioned that the indicia scanning capabilities of the postal authority will be utilized in a diverse number of new applications including both commercial transactions and enhanced service mail delivery, a sub-field within the message/memo field 60 (or some new field) will identify the particular indicia placed upon the postcard as bill payment indicia.

Detailed Description Text (58):
At stage 2, the customer 704, having opened the envelope from the vendor 700 and removed the postcard containing a payment authorization, submits the postcard to the postal authority 702. Prior to mailing the postcard the customer 704 may sign the postcard thereby authorizing payment of the bill. The signature may be either written or digital. However, the likelihood of fraud is low and therefore signatures of customers are not deemed essential. However, the digital signature of either the customer 704 or the vendor 700 greatly reduces the opportunity for fraud.

Detailed Description Text (59):
At stage 3, the postal authority 702 decodes the indicia on the postcard during the course of processing mail. The postal authority 702 first determines that the postcard represents a payment postcard. The postal authority 702 verifies the postcard's authenticity by performing a cryptographic transformation on the digital signature provided by the vendor 700. The postal authority 702 determines the parties to the bill payment transaction. A stages 4a and 4b the postal authority 702 issues credit/deposit and charge/debit instructions to the financial institutions (identified in the postal authority's database of enrolled users of postcard bill payment) of vendor 700 and the customer 704 respectively. Alternatively, the parties to the transaction maintain accounts with the postal authority and bill payments are applied to those accounts.

CLAIMS:

1. A method for negotiating value using cryptographically transformed electronically interpretable indicia media comprising the steps of:

issuing a value message including a payer identification, a payee identification, an amount to be negotiated by presentment to a postal authority outlet, and a payer digital signature;

providing a public key for cryptographically creating the payer digital signature in order to authenticate the value message;

presenting, by a payee, the value message to a postal authority outlet;

authenticating, by a postal authority validation apparatus, the value message by applying the public key to the digital signature; and

adjusting at least one account status to reflect successful completion of negotiating the value message.

2. A system for conveying value using cryptographically transformed electronically interpretable indicia media, the system comprising:

an electronic apparatus for generating a value message including a payer identification, a payee identification, an amount to be negotiated by presentment of the value message to a postal authority outlet, and a payer digital signature;

a public key for authenticating the value message by application of the public key to the payer digital signature;

a value message reader for sensing indicia within the value message and transmitting information within the value message in binary form;

a value message resolver including:

an electronic interface coupled to the value message reader for receiving the

information within the value message;

an authenticator for applying the public key, in accordance with a cryptographic transformation algorithm, to the payer digital signature to verify the authenticity of the value message; and

an account manager for adjusting at least one account status in response to successful cryptographic transformation and authentication of the value message by the authenticator.

Previous Doc Next Doc Go to Doc#